

Appl. No. 10/040,293  
Amdt. dated April 22, 2008  
Reply to Final Office Action of February 22, 2008

#### AFTER FINAL EXPEDITED PROCEDURE

This listing of claims replaces all prior versions, and listings of claims in the instant application:

#### Listing of Claims:

1. (Previously Presented) A method for managing identification in a data communications network, the method comprising:

receiving a portable user-controlled secure storage device;

enrolling a user of said portable user-controlled secure storage device with an authority network site, said enrolling comprising providing information requested by said authority network site;

receiving user data in response to said enrolling;

storing said user data in said portable user-controlled secure storage device;

enabling said portable user-controlled secure storage device to release said user data; and

using said user data, from said portable user-controlled secure storage device, at a service provider network site to obtain a service.

2. (Previously Presented) A method for managing identification in a data communications network, the method comprising:

receiving a portable user-controlled secure storage device;

enrolling a user of said portable user-controlled secure storage device with an authority network site, said enrolling comprising providing information requested by said authority network site;

receiving user data in response to said enrolling, said user data comprising a first portion and a second

GUNNISON, McKay &  
HODGSON, LLP  
Cotton Wood Office Plaza  
1901 Garden Road, Suite 220  
Mountain View, CA 94040  
(831) 433-0700  
Fax (831) 655-0888

Appl. No. 10/040,293  
Amdt. dated April 22, 2008  
Reply to Final Office Action of February 22, 2008

#### AFTER FINAL EXPEDITED PROCEDURE

portion, said first portion comprising a cryptogram  
computed based on said second portion;

storing said user data in said portable user-  
controlled secure storage device;

enabling said portable user-controlled secure storage  
device to release said user data; and

using said user data, from said portable user-  
controlled secure storage, at a service provider network  
site to obtain a service.

3. (Previously Presented) A method for managing  
identification in a data communications network, the method  
comprising:

presenting an identity credential request and data to  
be stored to a federated identity server via a client  
host;

receiving an identity credential in response to said  
identity credential request, said identity credential  
comprising a randomized ID and an identification authority  
ID, said federated identity server capable of verifying  
the truthfulness, accuracy and completeness of said data  
to be stored;

presenting a service request and said identity  
credential to a service portal, said service portal  
configured to issue an authentication request to said  
federated identity server;

receiving a logon credential in response to said  
service request, said login credential comprising an  
indication of the client host used by the user; and

using said logon credential to obtain a service from  
a service provider accessible via said service portal.

4. (Previously Presented) A computer program storage  
device including a tangible computer readable media having

GUNNISON, MCKAY &  
HODGSON, L.L.P.  
Garden West Office Plaza  
1501 Garden Road, Suite 220  
Menlo Park, CA 94025  
(415) 655-0888  
Fax (415) 655-0888

Appl. No. 10/040,293

Amdt. dated April 22, 2008

Reply to Final Office Action of February 22, 2008

#### AFTER FINAL EXPEDITED PROCEDURE

embodied therein a program of instructions executable by a processor to perform a method for managing identification in a data communications network, the method comprising:

receiving a portable user-controlled secure storage device;

enrolling a user of said portable user-controlled secure storage device with an authority network site, said enrolling comprising providing information requested by said authority network site;

receiving user data in response to said enrolling;

storing said user data in said portable user-controlled secure storage device;

enabling said portable user-controlled secure storage device to release said user data; and

using said user data, from said portable user-controlled secure storage device, at a service provider network site to obtain a service.

5. (Previously Presented) A computer program storage device including a tangible computer readable media having embodied therein a program of instructions executable by a processor to perform a method for managing identification in a data communications network, the method comprising:

receiving a portable user-controlled secure storage device;

enrolling a user of said portable user-controlled secure storage device with an authority network site, said enrolling comprising providing information requested by said authority network site;

receiving user data in response to said enrolling, said user data comprising a first portion and a second portion, said first portion comprising a cryptogram computed based on said second portion;

Appl. No. 10/040,293

Amdt. dated April 22, 2008

Reply to Final Office Action of February 22, 2008

#### AFTER FINAL EXPEDITED PROCEDURE

storing said user data in said portable user-controlled secure storage device;

enabling said portable user-controlled secure storage device to release said user data; and

using said user data, from said portable user-controlled secure storage device, at a service provider network site to obtain a service.

6. (Previously Presented) A computer program storage device including a tangible computer readable media having embodied therein a program of instructions executable by a processor to perform a method for managing identification in a data communications network, the method comprising:

presenting an identity credential request and data to be stored to a federated identity server via a client host;

receiving an identity credential in response to said identity credential request, said identity credential comprising a randomized ID and an identification authority ID, said federated identity server capable of verifying the truthfulness, accuracy and completeness of said data to be stored;

presenting a service request and said identity credential to a service portal, said service portal configured to issue an authentication request to said federated identity server;

receiving a logon credential in response to said service request, said login credential comprising an indication of the client host used by the user; and

using said logon credential to obtain a service from a service provider accessible via said service portal.

GUNNISON, McKay &  
HODGSON, L.L.P.  
Garden West Office Plaza  
1990 Garden Road, Suite 720  
Merced, CA 95340  
(931) 655-0888  
Fax (931) 655-0888

Appl. No. 10/040,293

Amdt. dated April 22, 2008

Reply to Final Office Action of February 22, 2008

#### AFTER FINAL EXPEDITED PROCEDURE

7. (Previously Presented) An apparatus for managing identification in a data communications network, the apparatus comprising:

means for receiving a portable user-controlled secure storage device;

means for enrolling a user of said portable user-controlled secure storage device with an authority network site, said enrolling comprising providing information requested by said authority network site;

means for receiving user data in response to said enrolling;

means for storing said user data in said portable user-controlled secure storage device;

means for enabling said portable user-controlled secure storage device to release said user data; and

means for using said user data, from said portable user-controlled secure storage device, at a service provider network site to obtain a service.

8. (Previously Presented) An apparatus for managing identification in a data communications network, the apparatus comprising:

means for receiving a portable user-controlled secure storage device;

means for enrolling a user of said portable user-controlled secure storage device with an authority network site, said enrolling comprising providing information requested by said authority network site;

means for receiving user data in response to said enrolling, said user data comprising a first portion and a second portion, said first portion comprising a cryptogram computed based on said second portion;

means for storing said user data in said portable user-controlled secure storage device;

GUNNISON, MCKAY &  
HODGSON, LLP.  
Cedrex West Office Plaza  
1001 Cedrex Road, Suite 220  
Menlo Park, CA 94025  
(831) 655-0880  
Fax (831) 655-0888

Appl. No. 10/040,293

Amdt. dated April 22, 2008

Reply to Final Office Action of February 22, 2008

#### AFTER FINAL EXPEDITED PROCEDURE

means for enabling said portable user-controlled secure storage device to release said user data; and

means for using said user data, from said portable user-controlled secure storage device, at a service provider network site to obtain a service.

9. (Previously Presented) An apparatus for managing identification in a data communications network, the apparatus comprising:

means for presenting an identity credential request and data to be stored to a federated identity server via a client host;

means for receiving an identity credential in response to said identity credential request, said identity credential comprising a randomized ID and an identification authority ID, said federated identity server capable of verifying the truthfulness, accuracy and completeness of said data to be stored;

means for presenting a service request and said identity credential to a service portal, said service portal configured to issue an authentication request to said federated identity server;

means for receiving a logon credential in response to said service request, said login credential comprising an indication of the client host used by the user; and

means for using said logon credential to obtain a service from a service provider accessible via said service portal.

10-18. (Cancelled)